The opinion in support of the decision being entered today is *not* binding precedent of the Board.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte RICHARD ALEXANDER HARRINGTON, RAMA I. SRINIVASAN, and TERENCE R. SPIES

Appeal 2007-1190
Application 09/288,462
Technology Center 2100

Decided: September 20, 2007

Before JAMES D. THOMAS, KENNETH W. HAIRSTON, and LEE E. BARRETT, *Administrative Patent Judges*.

HAIRSTON, *Administrative Patent Judge.*

DECISION ON APPEAL

Appellants appeal under 35 U.S.C. § 134 from a Final Rejection of claims 1 to 8. We have jurisdiction under 35 U.S.C. § 6(b).

We reverse.

STATEMENT OF THE CASE

Appellants have invented an installation module that has first and second versions of an encrypted software module. The first version of the encrypted software module is installed on a computing system if at least one of a set of trigger files is stored on the computing system. If at least one of the set of trigger files is not stored on the computing system, then the second version of the software module is installed on the computing system. The strength of encryption of the second version of the software module is less than the strength of encryption of the first version of the software module (Specification 11 to 13).

A decryption key to decrypt the encrypted software module is encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm (Specification 13).

Claim 1 is representative of the claims on appeal, and it reads as follows:

1. An installation module comprising:

an encrypted software module that is a first version of the software module;

a decryption key to decrypt the encrypted software module, wherein the decryption key is encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm; and

an executive for using the decryption key to decrypt the encrypted software module when at least one of a set of trigger files is stored on a computing system and to install the first version of the software module on the computing system when at least one of the set of trigger files is stored on the computing system, wherein each of the trigger files indicates authorization to install the encrypted software module, and wherein the first

version of the software module uses greater than a threshold strength encryption;

wherein a second version of the software module is installed if at least one of the set of trigger files is not stored on the computing system, and wherein the second version of the software module uses a strength encryption that is not greater than the threshold strength encryption.

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Scott	US 5,199,073	Mar. 30, 1993
Rubin	US 5,530,752	Jun. 25, 1996
Elgamal	US 5,825,890	Oct. 20, 1998
Davis	US 6,058,478	May 2, 2000 (filed Sept. 30, 1994)
Yoshida	US 6,075,862	Jun. 13, 2000 (filed Jul. 30, 1996)
Patel	US 6,192,474 B1	Feb. 20, 2001 (filed Jul. 31, 1998)
Chan	US 6,473,860 B1	Oct. 29, 2002 (filed Oct. 22, 1998)

The Examiner rejected claims 1 to 4, 6, and 8 under 35 U.S.C. § 103(a) based upon the teachings of Rubin, Yoshida, Chan, Davis, and Patel. The Examiner rejected claim 5 under 35 U.S.C. § 103(a) based upon the teachings of Rubin, Yoshida, Chan, Davis, Patel, and Scott. The Examiner rejected claim 7 under 35 U.S.C. § 103(a) based upon the teachings of Rubin, Yoshida, Chan, Davis, Patel, and Elgamal.

Appellants contend that "[a]s there is no discussion or mention of hashing the version number of Rubin or of why one would want to hash the

version number of Rubin, much less of using the hashed version number or of why one would want to use the hashed version number for encrypting the decryption key, Applicant respectfully submits that Rubin in view of Patel '474 cannot disclose or suggest wherein a decryption key is encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm as recited in claim 1" (Br. 9). Appellants conclude that "Yoshida, Chan, and Davis are not cited as curing, and do not cure, these deficiencies of Rubin in view of Patel '474" (Br. 9).

ISSUE

Does the applied prior art teach or would it have suggested to the skilled artisan a decryption key encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm?

FINDINGS OF FACT

As indicated *supra*, Appellants describe a decryption key that is encrypted "as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm."

Rubin describes a system and method for protecting a software program from unauthorized use and copying (Abstract; col. 2, ll. 7 to 9). Rubin protects a software program from unauthorized use and copying by removing up to the first four lines of code from each object code module of the program, and encrypting the removed lines of code in Encryption Conversion Process (ECP) 300 (Fig. 3; col. 5, ll. 13 to 22). The removed lines of code are encrypted by a bit-wise exclusive-or algorithm and a key randomly generated by ECP 300 (col. 5, ll. 32 to 39). The randomly

generated key is stored in Key 305 of a ROUND module 204 (col. 5, ll. 39 and 40). The encrypted lines of code are stored in a data area 205 of the module 204 (col. 5, ll. 21 and 22). The current version number of the associated routine is stored in Version Number 303 of the module 204 (col. 5, ll. 59 to 62).

In the decryption process in Rubin, the transformer 400 determines whether the Version Number 303 has been previously retrieved by comparing it with licensed versions numbers in temporary storage (col. 6, ll. 37 to 52). If the licensed version number is less than the Version Number 303, then the user is not licensed to use the software program (col. 6, ll. 53 to 55). If the licensed version number is greater than or equal to the Version Number 303[1], then the encrypted lines of code in module 204 are decrypted (col. 7, ll. 4 to 7). The transformer 400 performs the decryption by retrieving Key 305 and Encrypted Original Code 304 from module 204, and passing both through the bit-wise exclusive-or algorithm to thereby reproduce the originally lines of code for reintroduction into the software program (col. 7, ll. 10 to 17).

Patel describes a protocol for protecting over-the-air transfer of information from a mobile handset 20 and a network 10 (Fig. 3; col. 2, ll. 10 to 18). The protocol uses a Diffie-Hellman Encrypted Key exchange for establishing a secret key for the two parties over-the-air exchange (col. 2, ll. 29 to 35). A hash is used during a calculation (col. 3, ll. 31 to 35). If the hash is verified, then a key is established using the calculation results sent between the two parties (col. 3, ll. 35 to 38).

---

[1] The Version Number 303 functions as a trigger for the decryption process.

In Yoshida, a non-encrypted version of encrypted software demonstrates the software content that can be purchased on the encrypted version (col. 2, ll. 6 to 16). The encrypted version of the software can be decrypted with a key issued to an authorized user (col. 1, l. 66 to col. 2, l. 5).

Chan teaches that information can be encrypted at different levels of security (col. 1, ll. 41 to 53; col. 6, ll. 50 to 60).

Davis uses an encrypted key in a cryptographic device (Abstract; col. 3, ll. 55 to 59).

Scott was cited by the Examiner for "generating a hash value from the key value corresponding to database addresses (Col. 1, lines 11-16 & Col. 2, lines 3-10)" (Answer 6).

Elgamal was cited by the Examiner for disclosing "applications that employ a Winsock DLL in conjunction with the SLL library (Col. 12, lines 30-34)" (Answer 7).

PRINCIPLES OF LAW

The Examiner bears the initial burden of presenting a prima facie case of obviousness. *In re* Oetiker, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). The Examiner's articulated reasoning in the rejection must possess a rational underpinning to support the legal conclusion of obviousness. *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006).

"One cannot use hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention." *In re Fine*, 837 F.2d 1071, 1075, 5 USPQ2d 1596, 1600 (Fed. Cir. 1988).

In an obviousness rejection, it is impermissible "to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art." *In re Wesslau*, 353 F.2d 238, 241, 147 USPQ 391, 393 (CCPA 1965).

ANALYSIS

Although Rubin describes a version/trigger and a key used in a decryption process, and Patel uses a hash and a key during the protection protocol for over-the-air transfer of information between a mobile handset and a network, we agree with the Appellants' argument that "the mere discussion of using a hash of a value calculated as part of a Diffe-Hellman Encrypted Key Exchange as a session key in Patel '474 does not provide any disclosure or suggestion of hashing the version number of Rubin, much less of using the resulting hash value to encrypt a decryption key" (Br. 8). We also agree with the Appellants' argument that Yoshida, Chan, Davis, Scott and Elgamal do not cure the noted shortcoming in the teachings of Rubin and Patel (Br. 9 and 17).

CONCLUSION OF LAW

In the obviousness rejection, the Examiner used impermissible hindsight reconstruction to pick and choose among disclosures in the applied prior art references. Obviousness has not been established by the Examiner because the applied references neither teach nor would have suggested to the skilled artisan a decryption key "encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm."

ORDER

The obviousness rejections of claims 1 to 8 are reversed.

REVERSED

rwk

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE WA 99201